Data Breach Policy Report
EXECUTIVE SUMMARY

Purpose of Report: To provide to the School Board information regarding a recommendation to implement a data breach policy and accompanying regulation.

The goal of the Sioux Falls School District is to eliminate security incidents and avoid the breach of District data. The District currently has policy and follows best practice guidelines dealing with The Family Educational Rights and Privacy Act (FERPA) to help accomplish this. In 2018, South Dakota Senate Bill 62 introduced the requirement of mandatory reporting of the breach of personal information into South Dakota Codified Law within Chapter 22-40-19 to 22-40-26(Identity Crimes). Developing a data breach policy and regulation provides guidelines and expectations of what to do in the instance of a data breach by clearly defining the steps and action, thus, requiring all District employees to immediately report to the Director of Information and Technology Services when they know or suspect a breach of system security has occurred.

The regulation defines the critical terms, lays out the incident response and investigation steps, and outlines the notification procedures and content.

The District will continue to utilize best practice information and technology standards, policy, and education to protect personally identifiable information.

Administrative Recommendation to School Board: Acknowledge the Data Breach Policy Report.

Report Prepared by: Information & Technology Services May 13, 2019
Presented by: Michael Christopherson

SIOUX FALLS SCHOOL DISTRICT Policies and Regulations	NEPN Code: TBD

Data Breach of Personal or Protected Identifiable Information

The goal of the Sioux Falls School District is to eliminate security incidents and avoid any breach of District data. Thus, all District employees are required to immediately report to the Director of Information and Technology Services when they know or suspect that a breach of system security has occurred.

Policy adopted: tbd Board Action

	SIOUX FALLS SCHOOL DISTRICT	**NEPN Code: TBD**
	Policies and Regulations	

Definitions

Data Breach, Breach of Security or Breach – A security incident in which there was unauthorized access to and unauthorized acquisition of personal information maintained in computerized form that compromises the security, confidentiality or integrity of the information. A breach includes, but is not limited to, incidents in which personal or protected information has potentially been accessed without authorization or stolen; personal or protected information has been compromised; or a network hack or intrusion has occurred. Good-faith acquisition of personal information by a District employee or agent for a legitimate District purpose is not a breach of security provided that the personal information is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality or integrity of the personal information.

1. "Breach of system security," the unauthorized acquisition of unencrypted computerized data or encrypted computerized data and the encryption key by any person that materially compromises the security, confidentiality, or integrity of personal or protected information maintained by the information holder. The term does not include the good faith acquisition of personal or protected information by an employee or agent of the information holder for the purposes of the information holder if the personal or protected information is not used or subject to further unauthorized disclosure;

2. "Encrypted," computerized data that is rendered unusable, unreadable, or indecipherable without the use of a decryption process or key or in accordance with the Federal Information Processing Standard 140-2 in effect on January 1, 2018;

3. "Information holder," any person or business that conducts business in this state, and that owns or licenses computerized personal or protected information of residents of this state;

4. "Personal information," a person's first name or first initial and last name, in combination with any one or more of the following data elements:
   (a) Social security number;
   (b) Driver license number or other unique identification number created or collected by a government body;
   (c) Account, credit card, or debit card number, in combination with any required SDCL chapter 22-40 security code, access code, password, routing number, PIN, or any additional information that would permit access to a person's financial account;
   (d) Health information as defined in 45 CFR 160.103; or

(e) An identification number assigned to a person by the person's employer in combination with any required security code, access code, password, or biometric data generated from measurements or analysis of human body characteristics for authentication purposes.

5. "Protected information," includes:
   (a) A user name or email address, in combination with a password, security question answer, or other information that permits access to an online account; and
   (b) Account number or credit or debit card number, in combination with any required security code, access code, or password that permits access to a person's financial account;

6. "Unauthorized person," any person not authorized to acquire or disclose personal information, or any person authorized by the information holder to access personal information who has acquired or disclosed the personal information outside the guidelines for access of disclosure established by the information holder.

Incident Response

Once notified of an event, the Director of Information and Technology Services will identify and remedy the weakness that allowed the security incident to occur, to reasonably mitigate any harmful effects resulting from any privacy or security incident involving any District Data, minimize risk associated with the event, and determine who caused the incident. The investigation shall also include a determination on whether the incident was intentional or occurred because a user violated District policies, procedures or training, which may result in disciplinary action.

Data Breach

The District's primary goal when a breach of system security occurs is to recover as much data as possible, provide appropriate notifications of the breach of system security, and prevent further disclosure and harm to District students, employees and business operations.

The Director of Information and Technology Services will lead an investigation into the incident immediately to determine whether a breach occurred. If a breach occurred, the following steps will be taken as quickly as possible:

1. The Superintendent and other appropriate administrative staff will be notified immediately. The superintendent or designee will contact law enforcement when appropriate.

2. The Director of Information and Technology Services will determine the status of the breach and will take all appropriate measures to prevent additional loss of data and future breaches.

3. If possible, the Director of Information and Technology Services will preserve any and all evidence of the breach for future investigation, prosecution, insurance claims and other legal action.

4. District officials will determine the scope of the breach and will work with law enforcement (when appropriate) to determine whether District staff, impacted parents/guardians and students, or the public need to be notified and whether additional government agencies need to be involved.

5. Once the District's data has been secured, District officials will meet to evaluate the incident, determine the probable causes of the incident and determine what action should be taken to prevent future incidents.

Security Breach Notification

Breaches of confidential personal information are particularly problematic, and the District will take additional steps to prevent theft or fraud. The Director of Information and Technology Services will ensure that victims of security breaches are appropriately notified as required by law (SDCL chapter 22-40).

If the Director of Information and Technology Services, after an appropriate investigation or consultation with the relevant federal, state (notice to attorney general), or local agencies responsible for law enforcement, determines that identity theft or other fraud is not reasonably likely to occur as a result of the breach, such a determination shall be documented in writing and will be maintained for three years. If it is determined that identity theft is reasonably likely, the District will notify, without unreasonable delay, any person whose information may have been accessed.

This notice may be delayed if a law enforcement agency informs District that notification may impede a criminal investigation. Once the law enforcement agency communicates that notice may be provided, the notice will be provided without unreasonable delay.

If the District must provide notice to more than 250 residents, the District will also notify the Attorney General's Office. The District will report to these entities the timing, distribution, and content of the notice sent to the persons whose information may have been compromised.

Notice Content

The notice provided to persons whose information was breached shall minimally include:

1. A written notice of the incident in general terms.

2. A description of the type of personal information that was obtained as a result of the breach of security.

3. A telephone number that affected consumers may call for further information and assistance, if one exists.

4. Contact information for consumer reporting agencies as defined by law.

5. Advice that directs affected consumers to remain vigilant by reviewing account statements and monitoring credit reports.
6. Information about how to obtain a free credit report.

The notice may be made in writing or by e-mail if the person has agreed to receive communications from the District electronically in accordance with federal law. Telephone notice may be used if contact is made directly with the affected person.

Substitute notice may be used if the cost of providing notice would exceed $100,000 or if the District needs to notify more than 10,000 individuals. The District may also use substitute notice for individuals the District is unable to identify or for whom the District does not have sufficient contact information, but the District will use the regular notice for all other affected individuals.

Substitute notice shall include:
1. E-mail notice when the District has an e-mail address.
2. Conspicuous posting of the notice or a link to the notice on the District's website.
3. Notification to major statewide media.

Legal References:

Children's Internet Protection Act (CIPA) 29 USC § 6777; 45 CFR §54.520
Children's Online Privacy Protection Act (COPPA) 15 USC §6501-6506
Family Educational Rights and Privacy Act (FERPA) 20 U.S.C. 1232g; 34 C.F.R. Part 99
Protection of Pupil Rights Amendment 20 U.S.C. §1232h; 34 C.F.R. Part 98
Center for Internet Security - see http://www.cisecurity.org
Payment Card Industry/Data Security Standards (PCI/DSS) - see http://www.pcisecuritystandards.org

Related Policies/Regulations:
IJNDC/IJNDC-R – Acceptable and Ethical Use of Technology Resources
JRA/JRA-R – Student Records

Policy adopted: tbd

Board Action